



FEDERAL COMMUNICATIONS COMMISSION

[OMB 3060-XXXX; FR ID 50436]

Information Collection Being Reviewed by the Federal Communications Commission

AGENCY: Federal Communications Commission.

ACTION: Notice and request for comments.

SUMMARY: As part of its continuing effort to reduce paperwork burdens, and as required by the Paperwork Reduction Act of 1995 (PRA), the Federal Communications Commission (FCC or Commission) invites the general public and other Federal agencies to take this opportunity to comment on the following information collections. Comments are requested concerning: whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; the accuracy of the Commission's burden estimate; ways to enhance the quality, utility, and clarity of the information collected; ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology; and ways to further reduce the information collection burden on small business concerns with fewer than 25 employees. The FCC may not conduct or sponsor a collection of information unless it displays a currently valid Office of Management and Budget (OMB) control number. No person shall be subject to any penalty for failing to comply with a collection of information subject to the PRA that does not display a valid OMB control number.

DATES: Written PRA comments should be submitted on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. If you anticipate that you will be submitting comments but find it difficult to do so within the period of time allowed by this notice, you should advise the contact listed below as soon as possible.

ADDRESSES: Direct all PRA comments to Cathy Williams, FCC, via email to PRA@fcc.gov and to Cathy.Williams@fcc.gov.

FOR FURTHER INFORMATION CONTACT: For additional information about the information collection, contact Cathy Williams at (202) 418-2918.

SUPPLEMENTARY INFORMATION:

OMB Control Number: XXXX-XXXX.

Title: Section 20.23(b)(1), (3)-(5), (7); (c)(1)-(2), (3), (3)(iii)-(iv), (4)(i)-(ii), (v); and (d),
Contraband wireless devices in correctional facilities.

Form Number: N/A.

Type of Review: New information collection.

Respondents: Business or other for-profit entities, and state, local or tribal governments.

Estimated Number of Respondents and Responses: 531 respondents and 16,389 responses.

Estimated Time Per Response: 1 – 10 hours.

Frequency of Response: One-time application and self-certification response, one-time DCFO authorization request response, on occasion qualifying request response, on occasion reversal response, recordkeeping requirement, third party notification requirement.

Obligation to Respond: Required to obtain or retain benefits. Statutory authority for the currently approved information collection is contained in sections 1, 2, 4(i), 4(j), 301, 302, 303, 307, 308, 309, 310, and 332 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(j), 301, 302a, 303, 307, 308, 309, 310, and 332.

Estimated Total Annual Burden: 142,568 hours.

Total Annual Costs: No costs.

Nature and Extent of Confidentiality: Certain information collected during the CIS application and certification process will be treated as confidential from public inspection. To the extent necessary, respondents may request confidential treatment of information collected. See 47 CFR section 0.459.

Privacy Act Impact Assessment: No impact(s).

Needs and Uses: On July 13, 2021, the Commission released a Second Report and Order and Second Further Notice of Proposed Rulemaking, Promoting Technological Solutions to Combat Contraband Wireless Devices in Correctional Facilities, GN Docket No. 13-111, in which the Commission took further steps to facilitate the deployment and viability of technological solutions used to combat contraband wireless devices in correctional facilities. In the Second Report and Order, the Commission adopted a framework requiring the disabling of contraband wireless devices detected in correctional facilities upon satisfaction of certain criteria. The Commission further addressed issues involving

oversight, wireless provider liability, and treatment of 911 calls. Finally, the Commission adopted rules requiring advance notice of certain wireless provider network changes to promote and maintain contraband interdiction system effectiveness.

In establishing rules requiring wireless providers to disable contraband wireless devices in correctional facilities and adopting a framework to enable designated correctional facility officials (DCFOs) relying on an authorized Contraband Interdiction System (CIS) to submit qualifying requests to wireless providers to disable contraband wireless devices in qualifying correctional facilities, the Commission found that a rules-based process will provide a valuable additional tool for departments of corrections to address contraband wireless device use. The framework includes a two-phase authorization process: (1) CIS applicants will submit applications to the Wireless Telecommunications Bureau (Bureau) describing the legal and technical qualifications of the systems; and (2) CIS applicants will perform on-site testing of approved CISs at individual correctional facilities and file a self-certification with the Commission. After both phases are complete, DCFOs will be authorized to submit qualifying requests to wireless providers to disable contraband devices using approved CISs at each correctional facility. In addition, the Commission adopted rules requiring wireless providers to notify certain types of CIS operators of major technical changes to ensure that CIS effectiveness is maintained. The Commission found that these rules will provide law enforcement with the tools necessary to disable contraband wireless devices, which, in turn, will help combat the serious threats posed by the illegal use of such devices.

The new information collection in 47 CFR 20.23(b)(1) regarding the application to obtain new CIS certification will be used by the Bureau to determine whether to certify a system and ensure that the systems are designed to support operational readiness and minimize the risk of disabling a non-contraband device, and ensure, to the greatest extent possible, that only devices that are in fact contraband will be identified for disabling. Bureau certification will also enable targeted industry review of solutions by allowing interested stakeholders to provide feedback on the application for certification, including the proposed test plan.

The new collections in 47 CFR 20.23(b)(3) include the requirement that the CIS operator must file with the Bureau a self-certification that complies with paragraph (b)(3)(ii) of section 20.23, confirming that the testing at that specific correctional facility is complete and successful, and the CIS operator must serve

notice of the testing on all relevant wireless providers prior to testing and provide such wireless providers a reasonable opportunity to participate in the tests. Self-certification will help the Bureau to ensure that qualifying requests identify contraband wireless devices accurately and in accordance with legal requirements. In addition to being used by the Bureau, the self-certification will be relied upon by the DCFO in conjunction with qualifying requests for disabling at a particular correctional facility. The serving of notice to the wireless providers will give them awareness and an opportunity to participate in the process.

The new information collections in 47 CFR 20.23(b)(4) requires that wireless providers objecting to the certification filing submit objections to the Bureau within five business days and serve the DCFO and the CIS operator, which allows all stakeholders to participate in the process and raise objections. Section 20.23(b)(5) requires that CIS operators retest and recertify their systems at least every three years and comply with the same requirements as for initial self-certification. This requirement will enable the Bureau to ensure the ongoing accuracy and reliability of a given CIS at a particular facility. Section 20.23(b)(7) requires that a CIS operator retain records for at least five years and provide them upon request to the Bureau, which will support the Bureau's efforts to identify issues with CIS operations, resolve interference issues, and resolve complaints related to misidentification of contraband devices. The new collections in 47 CFR 20.23(c)(1)-(2) include the requirement that individuals that seek to be recognized on the Commission's DCFO list must send a letter to the Contraband Ombudsperson in order for the Commission to approve that person for the qualified DCFO list and provide certainty to wireless providers that disabling requests are made by duly authorized individuals. Qualifying requests that include the required information will be used by wireless carriers to prevent use of contraband devices on their network and on other wireless provider networks.

The new collections 47 CFR 20.23(c)(3)(iii)-(iv) provide that, upon receiving a disabling request from a DCFO, the wireless provider must verify the request, may reject the request and must notify the DCFO whether it is accepting or rejecting the request. This process ensures that a wireless provider responds to a DCFO within a reasonable timeframe—while giving the provider an opportunity to determine if there is an error—and to give the DCFO time to respond quickly if the request has been rejected. The wireless

provider may contact the customer of record to notify them of the disabling and involve them in the process.

The new collections in 47 CFR 20.23(c)(4) provide that a wireless provider may reverse a disabled device where it determines that the device was erroneously identified as contraband, and the wireless provider must notify the DCFO of the reversal. The wireless provider may choose to involve the DCFO in the review and reversal process. The DCFO must also provide notice to the Contraband Ombudsperson of the number of erroneously disabled devices. This process ensures the integrity of the contraband device disabling process by giving the wireless provider the opportunity to reverse a disabled device—with the ability to extend review to the DCFO—and by creating safeguards to make sure that the process is efficient and reliable.

The new collections in 47 CFR 20.23(d) regarding notification from CMRS licensees to MAS operators of technical changes to their network are required so that MAS operators are given sufficient time to make necessary adjustments to maintain the effectiveness of their interdiction systems. In order to ensure that issues regarding notification to solutions providers of more frequent, localized wireless provider network changes are appropriately considered, CMRS licensees and MAS operators must negotiate in good faith to reach an agreement for notification for those types of network adjustments not covered by the notice requirement. CMRS licensees must provide notice of technical changes associated with an emergency immediately after the exigency to ensure that MAS operators continue to be notified of network changes that could impact MAS effectiveness.

Federal Communications Commission.

Marlene Dortch,

Secretary,

Office of the Secretary.